

Data Processing Agreement

This Data Processing Agreement (“DPA”) is entered into between Crowdskills Ltd, incorporated and registered in England and Wales with company number 09050188 whose registered office is at Impact Hub, 34b York Way, Kings Cross, London N1 9AB trading as *Whitelance* ('the Processor'), and the Whitelance Customer ('the Controller').

This DPA shall set out the terms and conditions for the processing of personal data related to the services ('Services') provided by the Processor, to Controller under their main Subscription Agreement (“Main Agreement”).

Contents

1. Definitions
2. Nature and Objectives of Data Processing
3. Data Subject Rights
4. Data Subject Requests
5. Confidentiality
6. Disclosures of Personal Data
7. Security and Data Breaches
8. Data Transfers
9. Limitation of Liability
10. Audit Rights, Privacy Impact Assessments
11. Duration and Termination, Returning and Deletion of Personal Data
12. Governing Law and Dispute Resolution

1. Definitions

1.1 **“Applicable Data Protection Law”** means the UK Data Protection Legislation and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data including the General Data Protection Regulation ((EU) 2016/679) referred to as **“GDPR”**; the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended. In case of any conflict between UK and EU Data Protection Legislation, the Data Protection Legislation in force in European Union shall prevail.

1.2 Terms **“Controller”**, **“Processor”**, **“Sub-Processor”**, **“Data Subject”**, **“Personal data”** and **“Processing”** shall have the meaning given in Applicable Data Protection Law.

1.3 Term **“Services”** shall have the meaning of services provided by the processor.

2. Nature and Objectives of Data Processing

2.1 Processor has developed a platform-based service as defined in the Main Agreement. In order to provide the services that consist of matching service buyers with service sellers, personal data from the end-users will be collected, processed and stored. The Controller’s marketplace, provide by the Processor, will be the first entry point. By default, the Controller requests that the Processor collects the Personal Data as described in this Clause 2 for the main purpose of fulfilling the contract with Controllers’ end-users, and the Controller may re-define this data before or during their contract.

2.2 Personal data is processed to provide the processor’s core service to the subject, namely the provision of a freelance marketplace that facilitates contracts between freelancers and businesses.

2.3 The Data subject categories and types of personal data being processed are:

- Basic information such as name, age, postal address, email address and phone number
- Details about User’s employer (name, address, phone number, ID and VAT ID) should such information be considered to be personal data
- Authentication information such as username and password, and if any third party service (e.g. Facebook) is used to sign in, the user ID of that service
- Information relating to the customer relationship such as advertised profiles and services, job postings, related communications, agreed services, their start and end times and information on their use
- Billing information such as credit card number and expiration date, also processed by Processor’s payments processor (currently MangoPay, subject to change).

2.4 The following technical data is also automatically collected and processed:

- IP address
- Geographical location data based on the IP address
- Service access times
- Statistics on page views
- Any other automatically collected technical data

2.5 Furthermore, the Processor may also collect other anonymized statistics about the way the User uses the Services provided by the Processor.

2.6 Activities for which personal data is used:

2.6.1 Service. The main reason to collect personal data is to provide the Whitelance platform and Services, to issue accurate charges for the use of the Services and to manage the customer relationship. The processing of personal data in this case is based on the agreement between the Controller and the Processor. This concerns, for example, the data collected during the signing up for the Service, during the use of the Service and the technical data needed to run the Service in a secure manner and communications with Users.

2.6.2 Marketing and other communications. The Processor may occasionally send its Controllers (and End-Users when the relevant personal data has been collected by the Processor itself) email to inform about new features, solicit feedback, or provide information on what is going on with the Processor and its products, as well as the various marketplaces built using the Whitelance service. We base this on our legitimate interest to provide Users with relevant information as part of the Services and to promote our Services.

2.6.3 Service development and research. We always work to make our Services better. Therefore, we may use the User's data to improve the Services. We base this processing on our legitimate interest to grow and develop. The Processor may also collect technical data for statistical purposes to compile anonymous, aggregated statistics, such as about the most popular marketplaces. The Processor may display information publicly to others in an aggregate format that does not reveal statistics of any single marketplace. The Processor does not disclose personal data other than as described in the clauses below.

3. Data Subject Rights

3.1 In accordance with the applicable data processing law Processor will offer operational, technical or other measures to allow for Data Subjects to exercise their rights and freedoms.

4. Data Subject Requests

4.1 Processor will provide its assistance to enable the Controller to respond to any such requests under the applicable data processing law within the legally required time frame.

4.2 If such requests are made directly to the Processor, the Processor shall without undue delay inform the Controller and shall advise Data Subjects to file their requests to the Controller itself.

5. Confidentiality

5.1 Processor shall treat all Personal Data as confidential.

5.2 The Processor shall inform all its employees, agents and/or approved Sub-processors engaged in Processing the Personal Data about the obligation of confidentiality of the Personal Data.

5.3 Processor ensures that all Authorized persons shall process the Personal Data only as necessary for the performance of services.

6. Disclosures of Personal Data

6.1 Law. When required by law such as to comply with requests by competent authorities or in response to a subpoena, court order or other governmental request;

6.2 Protection. When we believe in good faith that disclosure is necessary to protect our rights, investigate fraud or to protect our Users' safety or rights.

6.3 Acquisition. If the Processor, or substantially all of its assets, are acquired, or in the unlikely event that the Processor goes out of business or enters bankruptcy, User information would be one of the assets that is transferred or acquired by a third party. You acknowledge that such transfers may occur, and that any acquirer of the Processor may continue to use your personal data as set forth in this Privacy Policy.

6.4 Sub-Processors. Processor is entitled to use subcontractors for the purposes of providing the Service under the Agreement. These subcontractors work on behalf of the Processor, and do not have an independent right to use the personal data disclosed to them. Processor discloses personal data to its subcontractors on a need to know basis when necessary to process such data on the Processor's behalf in order to provide Services. Subcontractors are subject to appropriate security and confidentiality requirements. The Controller hereby consents to the processor's use of subcontractors as described in this section. If the Controller objects when new subcontractors are added, the Controller shall have the right to terminate the Agreement by written notice before the effective date of the change. The Processor shall use its commercially reasonable efforts to reasonably ensure that its subcontractors are subject to equivalent requirements regarding confidentiality and data protection, as set out in this DPA. The Processors remains responsible for its subcontractors and their compliance with the obligations of this DPA. Sub-processors used by Processor are listed at Whitelance.co/subprocessors.

7. Security and Data Breaches

7.1 Processor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data. The Processor's security tools and processes include:

- Access Control: Only authorised administrators, users and applications have access to applications. Multi-Factor Authorisation is required for administrators.
- Monitoring and Logging: Every event is logged with AWS CloudTrail, and monitored via AWS CloudWatch.
- Encryption: All requests must be made via HTTPS, so data is encrypted in transit with Secure Sockets Layer (SSL) certificates. All user data is encrypted at rest with AES256 via AWS S3 and AWS DynamoDB.

7.2 Processor shall promptly notify the Controller when the processor or any sub-processors become aware of a Personal Data Breach affecting the Controllers personal data. Processor shall offer reasonable assistance for the Controller, and all information necessary for the Controller to evaluate the situation, and notify applicable data protection authorities and/or impacted end-users within 72 hour time-frame. Processor shall appoint a contact point with e-mail address and mobile phone number for Controller to contact in case of actual or alleged data breach.

8. Data Transfers

8. 1 Personal Data shall be processed outside of the European Economic Area by Processor or its subcontractor. If necessary, the Controller authorizes the Processor to enter into a data transfer agreement with its subcontractors incorporating relevant Standard Contractual Clauses in the name and on behalf of the Controller. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if Processor or its subcontractor has adopted alternative safeguards in accordance with Data Protection Regulation for the lawful transfer of Personal Data outside the EEA, such as Privacy Shield.

9. Limitation of Liability

9.1 Parties acknowledge and agree that under Applicable Data Protection Law there is no limitation of liability towards any damages for end-users nor finally awarded fines or other penalties imposed by competent authorities. However, between the Parties, neither party shall be liable for any indirect or consequential damages, including but not limited to loss of profits, sales or business opportunities, of the other Party arising under or in connection with this Agreement. This limitation of liability shall not apply to cases of intentional misconduct or gross negligence. It shall also not apply to claims from Data Subjects in damage caused by a breach of Applicable Data Protection Law, provided that:

9.1.1 The Processor is given prompt notice of any such claim;

9.1.2 The Controller provides reasonable co-operation to the Processor in the defense and settlement of such claim, at the Processor's expense; and

9.1.3 The Processor is given sole authority to defend or settle the claim.

10. Audit Rights, Privacy Impact Assessments

10.1 Processor may conduct a mutually agreed audit for the purposes of meeting its audit requirements regarding Personal Data processing. To request an audit the Processor shall request an audit at least four (4) weeks in advance of the proposed audit date. Audit shall be conducted by third party professional and reputable auditors that shall have reasonable access to service and personnel to conduct such an audit.

10.2 Processor will reasonably cooperate with the Controller to assist them in their privacy impact assessment, the Controller will pay for the Processor's reasonable relevant costs

11. Duration and Termination, Returning and Deletion of Personal Data

11.1 This DPA is will terminate upon the end of Services.

11.2 Users data will be processed from the time they register on the platform, until they request their profile to be deleted, except where data is required to be retained for legal reasons. Data relating to website non-user visitors are automatically deleted within 5 years from first entry.

11.3 Processor shall delete or return Personal Data to the Controller after the end of Services and shall delete existing copies unless applicable law requires storage of such data. In case the Controller demands that the Personal Data are returned to the Controller or to a third party, the Controller will pay for the Processor's reasonable costs and expenses arising out such return of the Personal Data.

12. Governing Law and Dispute Resolution

12. 1 This DPA shall be governed by the same laws and jurisdiction as the Main Agreement.

12. 2 In case of any conflict between the Main Agreement and this DPA, this DPA shall prevail for the subject matter of data protection.